LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~ apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus that a client does not have a valid session credential granted by the first ~~system~~apparatus;

after the determining, retrieving, at the first ~~system~~apparatus, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for ~~the~~ a second ~~system~~apparatus, the second ~~system~~ apparatus (1) grants session credentials based on successful authentication at the second ~~system~~apparatus, and (2) includes a protected resource on the second ~~system~~ apparatus that is accessible by the client; the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

the first ~~system~~ apparatus presenting at least some of the information from the session token to the second ~~system~~apparatus;

the first ~~system~~ apparatus inputting a determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus;

the first ~~system~~ apparatus effecting successful authentication to the client so as to

grant access, to the protected resource on the first ~~system~~apparatus, to the client based on the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus; and

directing the client to the first ~~system~~ apparatus to establish a session credential based on successful authentication at the first ~~system~~apparatus, after determining that the client does not have a valid session credential granted by the second ~~system~~apparatus.

2. (Currently Amended) A method according to claim 1, further comprising granting a session credential to the client by the first ~~system~~apparatus, after determining that the client has a valid session credential granted by the second ~~system~~apparatus.

3. (Currently Amended) A method according to claim 1, further comprising sending a session token to the client, the token corresponding to a session credential granted by the first ~~system~~apparatus.

4. (Currently Amended) A method according to claim 1, further comprising directing the client to the second ~~system~~ apparatus to establish a session credential based on successful authentication at the second ~~system~~apparatus, after determining that the client does not have a valid session credential granted by the second ~~system~~apparatus.

5. (Canceled).

6. (Currently Amended) A method according to claim 1, further comprising

maintaining the client session credential granted by the second ~~system~~apparatus.

7. (Canceled)

8. (Currently Amended) A method according to claim 1, wherein retrieving information from the session token held by the client comprises:

sending a query to the client from the first ~~system~~apparatus, the query including identification as originating from a domain name corresponding to the second ~~system~~apparatus; and

receiving a response to the query.

9. (Currently Amended) A method for validating session credentials of a client comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus that a client does not have a valid session credential granted by the first ~~system~~apparatus;

after the determining, retrieving, at the first ~~system~~apparatus, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for ~~the~~ a second ~~system~~ apparatus that grants session credentials based on successful authentication at the second ~~system~~apparatus, and the second

~~system~~ apparatus including a protected resource that is accessible by the client, the retrieving information from the session token held by the client comprises receiving a session token from the client corresponding to the second ~~system~~apparatus, and the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

presenting at least some of the information from the session token to the second ~~system~~apparatus;

determining whether the client has a valid session credential granted by the second ~~system~~apparatus, the determining whether the client has a valid session credential granted by the second ~~system~~ apparatus is at least partially from presenting information from the session token;

the first ~~system~~ apparatus inputting a determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus;

granting a session credential to the client on the first ~~system~~apparatus, after determining that the client has a valid session credential granted by the second ~~system~~apparatus;

sending a session token to the client, the session token corresponding to the session credential granted by the first ~~system~~apparatus, the session token allowing the client access to protected resources on the first ~~system~~apparatus, so as to provide successful authentication to the client; and

maintaining the client session credential; and

the first ~~system~~ apparatus inputting information from the second ~~system~~apparatus, and in response, the first ~~system~~ apparatus outputting, to the second ~~system~~apparatus, a determination that the first ~~system~~ apparatus has a valid session credential

for the client at the first ~~system~~apparatus, and

the second ~~system~~ apparatus effecting successful authentication so as to grant access, to the further protected resource on the second ~~system~~apparatus, to the client based on the determination from the first ~~system~~ apparatus that the client has a valid session credential with the first ~~system~~apparatus.

10. (Currently Amended) Computer executable software code stored on a non-transitory computer-readable medium and transmitted as an information signal, the code for validating credentials, the code comprising:

code to input, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

code to determine, at the first ~~system~~apparatus, that a client does not have a valid session credential granted by the first ~~system~~apparatus;

code to retrieve, after the determining that the client does not have a valid session credential granted by the first ~~system~~apparatus, at the first ~~system~~apparatus, information from a session token held by the client, the information corresponding to a session credential for ~~the~~ a second ~~system~~ apparatus that grants session credentials based on successful authentication at the second ~~system~~apparatus, the second ~~system~~ apparatus including a protected resource that is accessible by the client, and the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

code to present at least some of the information from the session token to the second ~~system~~apparatus; and

code to input, from the second ~~system~~ apparatus to the first ~~system~~apparatus, a determination whether the client has a valid session credential granted by the second ~~system~~apparatus; and

code to effect successful authentication so as to grant access to the protected resource on the first ~~system~~apparatus, to the client based on the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus; and

code to direct the client to the first ~~system~~ apparatus to establish a session credential based on successful authentication at the first ~~system~~apparatus, after determining that the client does not have a valid session credential granted by the second ~~system~~apparatus.

11. (Currently Amended) A non-transitory computer readable medium having computer executable code stored thereon, the code for validating credentials, the code comprising:

code to input, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

code to determine, at the first ~~system~~ apparatus that the client does not have a valid session credential granted by the first ~~system~~apparatus;

code to retrieve from the client, at the first ~~system~~ apparatus and after the

determining that the client does not have a valid session credential granted by the first ~~system~~apparatus, information from a session token held by the client, the information corresponding to a possible session credential for ~~the~~ a second ~~system~~ apparatus that grants session credentials based on successful authentication at the second ~~system~~ apparatus and that has a protected resource that is accessible by the client, the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

code to present at least some of the information from the session token to the second ~~system~~apparatus; and

code to input, from the second ~~system~~ apparatus to the first ~~system~~apparatus, a determination whether the client has a valid session credential granted by the second ~~system~~apparatus; and

code to effect successful authentication to the client so as to grant access to the protected resource on the first ~~system~~apparatus, to the client based on the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus.

12. (Currently Amended) A programmed computer for validating credentials, comprising:

a memory having at least one region for storing computer executable program code; and

a processor for executing the program code stored in the memory, wherein the program code comprises:

code to input, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system, the protected resource on the first system being accessible by the client only after successful authentication of the client at the first system;

code to determine, at the first system that the client does not have a valid session credential granted by the first system;

code to retrieve, at the first system and after the determining that the client does not have a valid session credential granted by the first system, information from a session token held by the client, the information corresponding to a session credential for ~~the~~ a second system that grants session credentials based on successful authentication at the second system, the second system including a protected resource that is accessible by the client, the protected resource on the second system being accessible by the client only after successful authentication of the client at the second system;

code to present at least some of the information from the session token to the second system; and

code to input, from the second system to the first system, a determination whether the client has a valid session credential granted by the second system and

code to effect successful authentication so as to grant access to the protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system;

code to direct the client to the first system to establish a session credential based on successful authentication at the first system, after determining that the client does not have a valid session credential granted by the second system;

code to input into the first system information from the second system, and in response, output from the first system, to the second system, a determination that the first system has a valid session credential for the client at the first system, and

code to effect successful authentication with the second system so as to grant access, to the further protected resource on the second system, to the client based on the determination from the first system that the client has a valid session credential with the first system.

13. (Currently Amended) A method for establishing session credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining at the first ~~system~~ apparatus that the client does not have a valid session credential granted by ~~a~~ the first ~~system~~apparatus;

determining that the client does not have a valid session credential granted by a second ~~system~~ apparatus based on successful authentication at the second ~~system~~apparatus;

sending, from the first ~~system~~ apparatus to the client, a log in page;

receiving, at the first ~~system~~ apparatus from the client, log in information;

sending, from the first ~~system~~ apparatus to the second ~~system~~apparatus, the log in information; and

after the determining at the first ~~system~~ apparatus that the client does not have a valid session credential granted by a first ~~system~~apparatus, receiving, at the first ~~system~~

apparatus from the second ~~system~~apparatus, information corresponding to a session credential granted by the second ~~system~~apparatus, the session credential granted by the second ~~system~~ apparatus based at least in part on the log in information and successful authentication at the second ~~system~~apparatus, the second ~~system~~ apparatus being one that (1) grants session credentials based on successful authentication at the second ~~system~~apparatus, and (2) includes a protected resource on the second ~~system~~ apparatus that is accessible by the client, the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus; and

the first ~~system~~ apparatus effecting successful authentication so as to grant access, to a protected resource on the first ~~system~~apparatus, to the client based on the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus;

the first ~~system~~ apparatus inputting information from the second ~~system~~apparatus, and in response, the first ~~system~~ apparatus outputting, to the second ~~system~~apparatus, a determination that the first ~~system~~ apparatus has a valid session credential for the client at the first ~~system~~apparatus, and

the second ~~system~~ apparatus effecting successful authentication so as to grant access, to the further protected resource on the second ~~system~~apparatus, to the client based on the determination from the first ~~system~~ apparatus that the client has a valid session credential with the first ~~system~~apparatus.

14. (Currently Amended) A method according to claim 13, further comprising granting a session credential for the first ~~system~~apparatus.

15. (Currently Amended) A method according to claim 13, further comprising granting a session credential for the second ~~system~~apparatus.

16. (Currently Amended) A method according to claim 13, further comprising associating session credentials for the first ~~system~~ apparatus and the second ~~system~~ apparatus with the client.

17. (Currently Amended) A method for establishing session credentials for a client, the method comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining that the client does not have a valid session credential granted by the first ~~system~~apparatus;

after the determining, retrieving, at the first ~~system~~apparatus, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for ~~the~~ a second ~~system~~appartus;

inputting information at the first ~~system~~apparatus, from the second ~~system~~apparatus, that the client does not have a valid session credential granted by the second ~~system~~apparatus, the second ~~system~~ apparatus including a protected resource, the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful

authentication of the client at the second ~~system~~apparatus;

sending, from the second ~~system~~ apparatus to the client, a log in page;

receiving, at the second ~~system~~ apparatus from the client, log in information; and

sending, from the second ~~system~~ apparatus to the first ~~system~~apparatus, information corresponding to a session credential granted by the second ~~system~~apparatus, the session credential granted by the second ~~system~~ apparatus based at least in part on the log in information and successful authentication at the second ~~system~~apparatus; and

granting a session credential to the client for the first ~~system~~ apparatus so as to provide successful authentication, such that the client is granted access to a protected resource on the first ~~system~~apparatus;

the first ~~system~~ apparatus inputting information from the second ~~system~~apparatus, and in response, the first ~~system~~ apparatus outputting, to the second ~~system~~apparatus, a determination that the first ~~system~~ apparatus has a valid session credential for the client at the first ~~system~~apparatus, and

the second ~~system~~ apparatus effecting successful authentication so as to grant access, to the further protected resource on the second ~~system~~apparatus, to the client based on the determination from the first ~~system~~ apparatus that the client has a valid session credential with the first ~~system~~apparatus.

18. (Currently Amended) A method according to claim 17, further comprising granting a session credential for the second ~~system~~apparatus.

19. (Currently Amended) A method according to claim 17, further comprising

associating session credentials for the first ~~system~~ apparatus and the second ~~system~~ apparatus with the client.

20. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus that a client does not have a valid session credential granted by the first ~~system~~apparatus;

redirecting the client to ~~the~~ a second ~~system~~ apparatus that grants session credentials based on successful authentication at the second ~~system~~apparatus, the second ~~system~~ apparatus having a protected resource that is accessible by the client;

sending, from the second ~~system~~ apparatus to the first ~~system~~apparatus, session credentials granted by the second ~~system~~apparatus;

sending, from the first ~~system~~ apparatus to the second ~~system~~apparatus, the session credentials granted by the second ~~system~~apparatus;

determining, at the second ~~system~~apparatus, that the session credentials granted by the second ~~system~~apparatus, and received from the first ~~system~~apparatus, are valid; and

sending, from the second ~~system~~ apparatus to the first ~~system~~apparatus, information indicating that the session credentials granted by the second ~~system~~ apparatus are valid; and

inputting, at the second ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the second

~~system~~apparatus;

determining, at the second ~~system~~ apparatus that a client does not have a valid session credential granted by the second ~~system~~apparatus;

after such determining, retrieving, at the second ~~system~~apparatus, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for the first ~~system~~apparatus;

redirecting the client to the first ~~system~~ apparatus that grants session credentials based on successful authentication at the first ~~system~~apparatus;

sending, from the first ~~system~~ apparatus to the second ~~system~~apparatus, session credentials granted by the first ~~system~~apparatus;

sending, from the second ~~system~~ apparatus to the first ~~system~~apparatus, the session credentials granted by the first ~~system~~apparatus;

determining, at the first ~~system~~apparatus, that the session credentials granted by the first ~~system~~apparatus, and received from the second ~~system~~apparatus, are valid; and

sending, from the first ~~system~~ apparatus to the second ~~system~~apparatus, information indicating that the session credentials granted by the first ~~system~~ apparatus are valid.

21.-22. (Canceled)

23. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first

~~system~~apparatus, the protected resource being accessible upon successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus that the client does not have a valid session credential granted by the first ~~system~~apparatus, so as to allow the client access to the protected resource on the first ~~system~~apparatus;

after the determining, retrieving, at the first ~~system~~apparatus, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for ~~the~~ a second ~~system~~apparatus;

the first system communicating with ~~a~~ the second ~~system~~apparatus, the second ~~system~~ apparatus having a further protected resource on the second ~~system~~apparatus, the further protected resource being accessible upon successful authentication of the client at the second ~~system~~apparatus;

the first ~~system~~ apparatus presenting information to the second ~~system~~apparatus;

the first ~~system~~ apparatus inputting a determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus;

the first ~~system~~ apparatus effecting successful authentication so as to grant access, to the protected resource on the first ~~system~~apparatus, to the client, based on the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus;

the first ~~system~~ apparatus inputting information from the second ~~system~~apparatus, and in response, the first ~~system~~ apparatus outputting, to the second ~~system~~apparatus, a determination that the first ~~system~~ apparatus has a valid session credential for the client at the first ~~system~~apparatus; and

the second ~~system~~ apparatus effecting successful authentication so as to grant access, to the further protected resource on the second ~~system~~apparatus, to the client based on the determination from the first ~~system~~ apparatus that the client has a valid session credential with the first ~~system~~apparatus.

24. (Canceled)

25. (Currently Amended) The method of claim 23, wherein the protected resource in the first ~~system~~ apparatus includes content provided on a pay-per-use basis, and wherein the protected resource in the second ~~system~~ apparatus includes content provided on a pay-per-use basis.

26. (Currently Amended) The method of claim 23, wherein the protected resource in the first ~~system~~ apparatus includes content provided on a subscription basis, and wherein the protected resource in the second ~~system~~ apparatus includes content provided on a subscription basis.

27. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus whether a client have a valid session

credential granted by the first ~~system~~apparatus;

retrieving, at the first ~~system~~apparatus, information from a session token held by the client if the client does not have a valid session credential granted by the first ~~system~~apparatus, wherein the information is retrieved from the client and the information corresponds to a session credential for a second ~~system~~apparatus, the second ~~system~~ apparatus (1) grants session credentials based on successful authentication at the second ~~system~~apparatus, and (2) includes a protected resource on the second ~~system~~ apparatus that is accessible by the client; the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

transmitting, at the first ~~system~~apparatus, at least some of the information from the session token to the second ~~system~~apparatus;

receiving and inputting, at the first ~~system~~apparatus, information associated with a determination from the second ~~system~~ apparatus whether the client has a valid session credential with the second ~~system~~apparatus, wherein the client's session credential with the second ~~system~~ apparatus is periodically renewed via the first ~~system~~apparatus;

effecting, at the first ~~system~~apparatus, successful authentication to the client so as to grant access, to the protected resource on the first ~~system~~apparatus, to the client based on the information associated with the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus; and

directing the client to the first ~~system~~ apparatus to establish a session credential, after the determination from the second ~~system~~ apparatus that the client does not have a valid session credential granted by the second ~~system~~apparatus.

28. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus whether a client have a valid session credential granted by the first ~~system~~apparatus;

retrieving, at the first ~~system~~apparatus, information from a first session token held by the client if the client does not have a valid session credential granted by the first ~~system~~apparatus, wherein the information is retrieved from the client and the information corresponds to a session credential for a second ~~system~~apparatus, the second ~~system~~ apparatus (1) grants session credentials based on successful authentication at the second ~~system~~apparatus, and (2) includes a protected resource on the second ~~system~~ apparatus that is accessible by the client; the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system~~apparatus;

transmitting, at the first ~~system~~apparatus, at least some of the information from the first session token to the second ~~system~~apparatus;

receiving and inputting, at the first ~~system~~apparatus, information associated with a determination from the second ~~system~~ apparatus whether the client has a valid session credential with the second ~~system~~apparatus, wherein the client's session credential with the second ~~system~~ apparatus is periodically renewed via the first ~~system~~apparatus;

effecting, at the first ~~system~~apparatus, successful authentication to the client so as to grant access, to the protected resource on the first ~~system~~apparatus, to the client based on

the information associated with the determination from the second ~~system~~ apparatus that the client has a valid session credential with the second ~~system~~apparatus; and

directing the client to the first ~~system~~ apparatus to establish a session credential, after the determination from the second ~~system~~ apparatus that the client does not have a valid session credential granted by the second ~~system~~apparatus, wherein the step of directing the client to the first ~~system~~ apparatus to establish a session credential further comprises:

receiving, at the first ~~system~~apparatus, a redirect code in response to the determination from the second ~~system~~ apparatus that the client does not have a valid session credential granted by the second ~~system~~apparatus;

directing the client to a log in page provided by the second ~~system~~ apparatus based on the redirect code;

receiving, at the first ~~system~~ apparatus from the client, log in information;

sending, from the first ~~system~~ apparatus to the second ~~system~~apparatus, the log in information; and

receiving, at the client, a second session token if the second ~~system~~ apparatus determines that the log in information is valid.

29. (Currently Amended) A method for validating credentials comprising:

inputting, at a first ~~system~~ apparatus that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first ~~system~~apparatus, the protected resource on the first ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the first ~~system~~apparatus;

determining, at the first ~~system~~ apparatus whether a client have a valid session

credential granted by the first ~~system~~apparatus;

generating a log in page at the first ~~system~~ apparatus and present the log in page to the client, wherein the log in page corresponds to a second ~~system~~apparatus, the second ~~system~~ apparatus (1) grants session credentials based on successful authentication at the second ~~system~~apparatus, wherein the session credentials of the second ~~system~~ apparatus is periodically renewed via the first ~~system~~apparatus, and (2) includes a protected resource on the second ~~system~~ apparatus that is accessible by the client; the protected resource on the second ~~system~~ apparatus being accessible by the client only after successful authentication of the client at the second ~~system;~~apparatus;

receiving, at the first ~~system~~ apparatus from the client, authentication credentials required by the log in page;

transmitting, from the first ~~system~~ apparatus to the second ~~system~~apparatus, the authentication credentials required by the log in page; and

generating, at the first ~~system~~apparatus, one or more session tokens for the first ~~system~~ apparatus and the second ~~system~~ apparatus if the second ~~system~~ apparatus determines that the authentication credential required by the log in page is valid, wherein the one or more session tokens for the first ~~system~~ apparatus and the second ~~system~~ apparatus grant access, to the protected resource on the first ~~system~~ apparatus and to the protected resource on the second ~~system~~apparatus.